The Gideons International

P.O. Box 140800
Nashville, TN 37214

www.gideons.org
PH 615.564.5000
FX 615.564.6000

September 15, 2020

Attorney General Wayne Stenehjem
Office of the Attorney General
Consumer Protection and Antitrust Division
600 E. Boulevard Ave. Dept. 125
Bismarck, ND 58505

Re: Notice of Security Incident Regarding The Gideons International

Dear Attorney General Stenehjem:

I write to inform you of a recent security breach that affected The Gideons International ("Gideons"). Blackbaud, Inc. ("Blackbaud") is a third-party service provider for Gideons, which provides support for donor engagement and development activities. Blackbaud experienced a ransomware attack and recently notified Gideons that its donor information was affected by Blackbaud's security incident.

After review of the affected donor information, Gideons determined that there were North Dakota residents whose date of birth information was disclosed in conjunction with their names. As a result, Gideons sent the attached notification of the security incident to the affected [insert number] North Dakota residents.

Please contact me directly at ssiple@gideons.org or 615-564-5200 if you have any questions or if you need any additional information.

Sincerely,

Samuel D. Siple

Samuel D. Siple
Chief Program Advancement Officer

202410

Date

«FirstName» «LastName»
«AddressLine1»
«AddressLine2»
«City», «State» «Zip»

Notice of Data Breach

Dear «Salutation»,

We are writing to let you know about a data security incident, which may have involved your personal information. The Gideons International takes the protection and proper use of your information seriously. Therefore, we are contacting you to explain the incident and provide you with steps you can take to protect yourself.

What Happened

Recently, Blackbaud, Inc. a third-party service provider of The Gideons, notified us that they had discovered and stopped a ransomware attack in May of 2020. After discovering the attack, the Blackbaud's Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking their access and fully encrypting database files; and ultimately expelled them from their system. However, prior to locking out the cybercriminal, the cybercriminal removed a copy of a subset of data, which included a portion of The Gideons' donor information.

According to communication from Blackbaud, they paid to have the data destroyed by the attacker and not transferred. Blackbaud communicated it has no reason to believe that any data went beyond the cybercriminal, was or will be misused, or will be disseminated or otherwise made publicly available.

What Information Was Involved

Blackbaud informed us that donors' Social Security numbers, credit or debit card numbers, bank account information, and any usernames or passwords contained in the database were encrypted and not at risk of compromise.

We reviewed the unencrypted data that was compromised and determined that data may have included name (including maiden name and nickname), spouse name, marital status, gender, date of birth, address, employment relationships, and history of your relationship with The Gideons. However, not all data fields were disclosed for each donor.

What We Are Doing

The Gideons International values your privacy and deeply regrets that this incident occurred. We are notifying you so that you can take immediate action to protect yourself. We are also notifying the North Dakota Attorney General in accordance with state laws. To prevent something like this from happening in the future, Blackbaud has indicated they have already implemented several changes to protect your data from any subsequent incident.

What You Can Do

As a best practice, we recommend you stay vigilant for incidents of fraud and identity theft by reviewing account statements for unauthorized activity, and promptly report any suspicious activity or suspected identity theft to us and to the proper authorities.

Please see the "Recommended Steps to Help Protect Your Information" below for information on additional steps you can take.

For More Information

We continue to trust the Lord as our ultimate protector and provider, thankful for faithful supporters like you. We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have any further questions or concerns regarding this matter, please contact The Gideons' Development Director, Matthew Work, at 615-564-5090 or mwork@gideons for more information.

Sincerely,

Samuel D. Siple

Samuel D. Siple
Chief Program Advancement Officer

Recommended Steps to Help Protect Your Information

1. Review your credit reports. Under federal law, you are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

2. Place Fraud Alerts with the three credit bureaus. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only one of these bureaus and use only one of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

3. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

4. You can obtain additional information about the steps you can take to avoid identity theft from the following agency:
Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.